European Commission

Recommended practices to enhance cybersecurity in transport organisations

There are a substantial number of cyber threats targeting transport services and systems. You can help to protect your organisation by following cybersecurity good practices addressing common emerging threats across all modes of transport. In case of doubts, contact your local information security officer or responsible.

Protect against malware infections

- Protect all systems with **strong passwords** and encryption
- **Backup your data** regularly into secure and authorised data storage devices or services
- Avoid opening attachments and clicking on hyperlinks of **unexpected emails** and suspicious popup windows
- Avoid using untrusted or **unknown removable devices** such as USB sticks, hard disks, and other storage devices
- Install and update regularly authorised software, and avoid disabling security software measures

Help to identify denial of service attacks

You should contact or report immediately to your local information security officer, if you experience any of the following situations:

- **Slow degraded services** and responses due to increasing requests of memory, computing and network resources
- **Unexpected behaviours** of services and systems such as frequent crashes and error messages
- Unexpected network connections or loss of connections to services and systems

Avoid unauthorised access and theft by protecting your data

- Never share or publish your **credentials and personal data**, including pictures or social media posts that may reveal such information
- Protect sensitive data typed on keyboards or shown on screens from unauthorised individuals
- Use **complex passwords** (e.g. sufficiently long password combining alphanumerical and special characters)
- **Change default passwords** and use different credentials for all connected services, systems and devices
- Activate **Two-Factor Authentication**, if possible

Be aware of software manipulation

- Install and download only software and updates from **trusted suppliers**, sources and websites for all systems and devices (including personal computers, servers, peripherals, network devices, smartphones, etc.)
- Scan any software and storage devices with a reliable and **updated antivirus**
- **Uninstall unnecessary or not recently used software**, and disable unnecessary connections (e.g. network protocols and services) including access to remote services (e.g. cloud storage services)